

# **Document made available under the Patent Cooperation Treaty (PCT)**

International application number: PCT/JP05/006588

International filing date: 04 April 2005 (04.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-114639  
Filing date: 08 April 2004 (08.04.2004)

Date of receipt at the International Bureau: 20 May 2005 (20.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2004年 4月 8日

出願番号 Application Number: 特願 2004-114639

パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is

出願人 Applicant(s): 三菱電機株式会社

J P 2004-114639

特許庁長官  
Commissioner,  
Japan Patent Office

2005年 4月 27日

小川



【書類名】 特許願  
【整理番号】 550007JP01  
【提出日】 平成16年 4月 8日  
【あて先】 特許庁長官殿  
【国際特許分類】 G01S 5/14  
【発明者】  
【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内  
【氏名】 斎藤 謙一  
【特許出願人】  
【識別番号】 000006013  
【氏名又は名称】 三菱電機株式会社  
【代理人】  
【識別番号】 100099461  
【弁理士】  
【氏名又は名称】 溝井 章司  
【手数料の表示】  
【予納台帳番号】 056177  
【納付金額】 16,000円  
【提出物件の目録】  
【物件名】 特許請求の範囲 1  
【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1

## 【書類名】特許請求の範囲

### 【請求項 1】

測位衛星からの測位コードと搬送波とを自身の識別符号で暗号化して測位端末から送信された伝送データを受信して、

上記測位端末の識別符号を記憶して、該識別符号で上記伝送データを復号化する復号化部と、

上記復号化部によって復号化された測位コードと搬送波とに基づいて上記測位端末の位置を演算する位置演算部と、

上記位置演算で得られた位置情報を証明する証明書生成部とを備えて、

端末から位置保証要求があると、該当する上記位置演算による位置情報の証明を行うことを特徴とする位置保証サーバ。

### 【請求項 2】

他の位置を示す装置の情報と、時刻を示す情報とのうちから 1 つを付加して位置情報を証明することを特徴とする請求項 1 記載の位置保証サーバ。

### 【請求項 3】

測位衛星からの位置情報に対する補正情報に基づく演算と、測位衛星の配置情報との内から 1 つを付加して位置情報を証明することを特徴とする請求項 1 記載の位置保証サーバ。

### 【請求項 4】

測位衛星からの測位コードと搬送波とを自身の識別符号で暗号化して伝送データを送信する測位端末と、

上記測位端末の識別符号を記憶して、上記伝送データを受信して復号化する復号化部と、該復号化した測位コードと搬送波とに基づいて上記測位端末の位置を演算する位置演算部と、該位置演算で得られた位置情報を証明する証明書生成部とを備えて、端末から位置保証要求があると、該当する上記位置演算による位置情報の証明を行うサーバ、とで構成されることを特徴とする位置保証システム。

### 【請求項 5】

測位端末は、測位衛星からの測位コードと搬送波とを受信する部分と、該受信した信号を自身の識別符号で暗号化する部分を耐タンパ化したことを特徴とする請求項 4 記載の位置保証システム。

### 【請求項 6】

測位端末において、測位衛星からの測位コードと搬送波とを自身の識別符号で暗号化して伝送データとして送信するステップと、

サーバにおいて、記憶している上記測位端末の識別符号を用いて上記伝送データを受信して復号化するステップと、

上記復号化した測位コードと搬送波とに基づいて上記測位端末の位置を演算するステップと、

位置保証要求があると、上記位置演算ステップで得られた位置情報を証明する証明書生成ステップ、とを備えたことを特徴とする位置保証方法。

【書類名】明細書

【発明の名称】位置保証サーバ、位置保証システム及び位置保証方法

【技術分野】

【0001】

この発明は測位衛星情報等を用いた位置認証に関するシステム、機器についてのものである。

【背景技術】

【0002】

従来から、携帯端末等の移動体の位置を特定して、その位置を保証するシステムがある。特許文献1に記載された従来の位置保証システムでは、3つ以上の測位衛星からの情報を使用したGPS(Global Positioning System)等を利用して得られた位置情報や時刻情報自体を認証している。その構成として、測位端末(デジタルカメラ)は、GPSレシーバで受信したGPS電波から生成した経度／緯度情報を暗号化し、位置情報としてサーバに送信する。サーバはその位置情報を復号化し、得られた経度／緯度情報から場所特定データを生成し、コピーガード処理して測位端末へ送信する。このことにより、他の場所で撮影されたものではないことが証明される。

しかしこのシステムでは、移動体端末であるGPSレシーバにおいて、位置を算出する機能を持つように構成されているため、一般的なGPSレシーバが持つ問題を同様に持つことになる。

【0003】

一般的なGPSレシーバ100は、図10に示すように、GPS衛星からの電波を受信するGPSアンテナ101と、GPSアンテナ101が受信したアナログ信号をデジタル信号に変換する受信装置102、及びデジタル信号から取り出される測位コード111、搬送波112などを用いて位置を算出する位置演算装置103から構成され、複数のGPS衛星から受信した電波を用いて位置(緯度、経度など)を生成する。

このGPSレシーバ100は、例えば測位においてコールドスタート(電源投入後最初の測位)に、例えば数十秒程度の時間がかかるという問題があり、ユーザからの要求が出てから位置を算出できるようになるまでの上記の時間は、証明を受けることができない。

また当然のことながら、GPS信号が受信できない場所では測位ができないため、そのような場所では証明を受けることができない。

更に、例えばGPSシミュレータのように、GPSアンテナの出力と同様の出力を発生可能な機器を用いれば、GPSレシーバに誤ったGPSアンテナの出力を入力することが可能である。また情報処理装置に誤った位置を直接入力することも可能である。

【0004】

更に、民間が利用可能なGPS測位の方式としては、大きく分けて、測位コード(C/Aコード)を用いる方法と、搬送波の位相を用いる方法とがあるが、このうち測位コードは容易に偽造可能であることが知られて入る。例えば、Pseudoliteのように、GPS衛星と同じ信号を発生可能な機器をアンテナの近傍に設置することで、GPSアンテナに誤ったGPS信号を入力することが可能である。

いずれの場合にも、実際に測位端末が居た位置と異なる位置がセンターシステム(サーバ)に通知される可能性があるが、サーバではそれを検知することはできないため、その通知された誤った位置に対し証明を与えてしまうことになる。

【特許文献1】特開2001-33537号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

従来の位置保証システムは上記のように構成されており、位置保証までに時間がかかる場合がある、または位置保証ができない、という課題がある。

また従来システムでは、デジタルカメラまたは測位端末で位置または経度と緯度を算出するように構成されているため、誤った情報を容易に混入させることが可能である、と

いう課題がある。

更に、意図的に端末から誤った位置情報を送信しても、サーバでその誤った位置に対して認証を与えててしまう、という課題がある。

更に、一般的にG P Sによる測位では数メートルから数十メートル程度の誤差を含む可能性があることが知られているが、一般的なG P Sシステムに基づいて証明された位置が必ずしも正確な位置であるとは保証ができない。

#### 【0006】

本発明は上記の課題を解決するためになされたもので、コールドスタート時間が短い位置保証を得る、またG P S信号が受信できない場所での位置保証を実現することを目的とする。

また本発明の別の目的は、誤った情報の混入の防止、及び検出を行い、信頼性の高い位置保証を実現することである。

更に本発明の別の目的は、位置の精度を明らかにした位置保証を実現することである。

#### 【課題を解決するための手段】

##### 【0007】

この発明に係るサーバは、測位衛星からの測位コードと搬送波とを自身の識別符号で暗号化して測位端末から送信された伝送データを受信して、

上記測位端末の識別符号を記憶して、この識別符号で上記伝送データを復号化する復号化部と、上記復号化部によって復号化された測位コードと搬送波とに基づいて上記測位端末の位置を演算する位置演算部と、上記位置演算で得られた位置情報を証明する証明書生成部とを備えて、

端末から位置保証要求があると、該当する上記位置演算による位置情報の証明を行うことを特徴とする。

#### 【発明の効果】

##### 【0008】

この発明によれば測位コードと搬送波とを暗号化した入力を、サーバにおいて復号し、位置演算するので、改ざんが出来にくく、かつ即時応答が可能で、信頼性が高い位置保証が得られる効果がある。

#### 【発明を実施するための最良の形態】

##### 【0009】

実施の形態1.

位置保証を要求して、直ちに保証が得られ、かつ保証の正しさが高い位置保証装置、システムを説明する。

なお、こうした位置保証サービス提供システムとして図2に示すシステムの例としては、ある車が課金エリア内に居たことを証明するロードプライシングシステムや、機密文書閲覧可能区域に居ることを証明する情報セキュリティ・システムなどがある。こうした位置保証システムでは、G P S信号を受信し、ある時刻に、ある位置にいたことの位置保証を要求する、または更にその位置精度情報の保証を要求する測位端末10と、その要求を受けて、それらを保証する証明書を発行する位置保証サーバ20(以降サーバと記述)と、そして、発行された証明書を利用する利用端末30が、無線通信網やインターネットなどの有線通信網などの通信網を通して接続される構成をとる。なお、利用端末30は測位端末10と同一の端末であっても構わない。例えば測位端末10としては専用端末の他、携帯電話、P D A、カーナビなどの携帯端末が考えられ、歩行者が携帯端末を持つ場合、もしくは自動車や二輪車などに搭載される場合がある。

またサーバは、位置保証センタなどに設置される。

##### 【0010】

本実施の形態におけるシステムのハードウェア構成を図1に示す。

先ず測位端末10は、以下の構成要素からなる。即ち、G P S信号である測位コード111と搬送波112を受信するG P Sアンテナ11と、この受信したG P Sアンテナ11で受信した信号、搬送波に関してはA／D変換した信号を、伝送用データに変換するA／

D付受信部12と、測位端末ごとに割り振られた固有の識別記号(ID)を記憶するID記憶部15と、伝送用データを上記IDを用いて暗号化する暗号化部14と、暗号化された伝送用データをサーバに送信する通信部16と、サーバから送られてくる位置保証を記憶する保証記憶部17とで構成される。

サーバ20は、以下の構成要素からなる。暗号化された伝送用データを受信し、位置保証を送信する通信部21と、暗号化された伝送用データを復号化する復号化部23と、復号化された伝送用データから位置を算出する位置演算部24と、算出された位置に対する証明書(位置保証)を作成する証明書生成部22である。位置保証は、必要に応じてコピーガードを施して、受信側において違法なコピーが出来ない様にしておくこともできる。

#### 【0011】

図2のシステム図と、図3の動作フロー図に基づいて、システム全体の処理の流れは、以下の通りとなる。

(1) 測位端末10は、GPSアンテナ11で測位コード111と搬送波112との組を受信し、A/D付受信部12は、これをデジタル信号にする。これは複数の測位衛星から受信して、測位衛星の識別記号と共に組として信号とする。そして暗号化部14は、この測位コード111と搬送波112と測位衛星識別番号とを、自身のIDを用いて暗号化する。この暗号化には一般に知られている方式が利用出来る。そしてS41で、その暗号化出力を、位置保証要求と共にサーバ20に送信する。

(2) サーバ20は、S31において通信部21で位置保証要求を受けると、S32において復号化部23で送信された信号を復号化する。この復号化には一般に知られている方式が利用出来る。S33において位置演算部24で、この復号された測位コード111と搬送波112と測位衛星識別番号に基づいて、送信してきた測位端末10の位置と時刻を算出する。そして測位端末10のIDと共に証明書生成部22に渡す。この位置算出計算は、一般に知られている方式が利用出来る。

(3) そしてサーバ20は、S34でサーバの証明書生成部22において、受け取った信号に基づく位置と時刻を、端末に固有のIDに対する証明書として作成する。この証明書にコピーカードを施すことで改ざん不可能なものとするが、その作成方式は一般に知られている方式が利用出来る。この作成した位置保証の証明書を利用端末に送信する。

#### 【0012】

位置を演算するためには、その時点でのGPS衛星の位置を知る必要がある。測位端末10にて衛星の位置を知る方法としては、GPS信号から取り出す方法の他に、ネットワークアシスト型と呼ばれるサーバから取得する方法などがある。しかしいずれもコールドスタート時には、演算できるようになるまでにかなりの時間がかかる。

これに対して上記の構成によれば、サーバ20で位置の演算を行うため、測位端末のコールドスタート時間を短くできる効果がある。また更に、測位コードと搬送波を暗号化して送信するので、位置情報の改ざんが出来難いという効果もある。

#### 【0013】

実施の形態2.

位置情報の改ざんをより出来難くしたシステムを説明する。

本実施の形態におけるシステム構成を図4に示す。ハードウェア構成は図1の構成と同様であるが、サーバ20が受ける位置と時刻情報は、測位端末10bからのGPS信号のみでなく、測位端末10bが通信網と接続する基地局40の位置と時刻情報も受ける。

#### 【0014】

この構成におけるシステムの動作は、ほとんど実施の形態1と同様に動作するが、異なるところは以下の部分である。

サーバ20は、端末から位置保証要求を受けると、送信されたGPS信号及び同時に受信した通信ネットワーク上の位置、例えば携帯電話であればその携帯電話が通信に利用している基地局40が通信ネットワーク上の位置となり、その受信した位置情報から通信ネットワークの位置と時刻も算出する。

サーバ20は、端末からの位置保証要求に対して、ネットワーク位置も加えた位置保証

を出力する。

#### 【0015】

通信ネットワーク上の位置、この場合の基地局40は、端末で改ざんすることが不可能である。従ってサーバ20での位置の算出にネットワーク上の位置記載を併用することにより、より信頼性高く位置を保証でき、改ざんを防ぐ効果がある。

更に、位置の算出に通信ネットワーク上の位置を利用するので、算出するための必要な数のGPS信号を受信できていない場合でも、位置を保証できる効果がある。

#### 【0016】

本実施の形態における他のシステム構成を図4に基づいて説明する。

図において、測位端末10bは、準天頂衛星51や携帯電話基地局40などから無線通信や放送などの方法によって配布される時刻を得る。また測位端末10bは、図5に示すこれらの時刻を受信する時刻証明受信部18を備える。

#### 【0017】

上記図4と図5のシステムの動作で、これまでの実施の形態と異なる部分は、以下の点である。

(11) 測位端末10bは、受信したGPS信号と、時刻証明受信部で受信した準天頂衛星や携帯電話基地局からの時刻情報と、位置保証要求をサーバに送信する。

(12) サーバ20は、端末からの位置保証要求を受けると、送信された信号を復号化し、GPS信号からその位置と時刻を算出し、かつ受信した時刻情報の時刻とを比較する。そして時刻の正当性を検証する。

#### 【0018】

このように、例え一度他のアンテナで受信したGPS信号がある時間が経過した後に再送出することにより位置を成りますような場合を検出できる。従って、この構成によれば、より信頼性の高い位置保証が可能である。

#### 【0019】

更に他のハードウェア構成を図6に基づいて説明する。

図において、測位端末10cは、耐タンパ化部31を備える。即ち測位端末10cのGPSアンテナ11、受信部12、暗号化部14、ID記憶部15（必要に応じて時刻証明受信部18）、が分解不可能なように耐タンパ化されている。システム構成は、他のシステム構成と同様である。

動作は他のシステムと同様であるので、詳細記述は省略する。

この構成によれば、例えはGPSシミュレータのようにGPSアンテナの出力と同様の出力を発生する機器を用いて誤った信号を入力することにより、位置を成ります場合を防ぐ効果がある。従って、より信頼性の高い位置保証が可能である。

#### 【0020】

実施の形態3.

端末の位置情報自体の精度を高めた位置保証システムを説明する。

本実施の形態におけるシステム構成は図2と同様である。またハードウェア構成を図7に示す。本構成はサーバ20d側に、復号化された伝送用データと算出された位置、時刻を関連付けて記録する信号蓄積部25と、信号蓄積部25に記録された情報を用いて復号化されたデータに混入している不要な信号を除去する信号除去部26、とを備えている。

#### 【0021】

この構成における動作は、ほとんどが実施の形態1と同様であるが、以下の動作が加わる。

サーバの復号化部23が復号化した伝送データと、同時に取り出された測位端末10のIDとを信号除去部26に出力する。サーバの信号除去部26は、受け取った伝送用データから混入された不要な信号を除去し、端末のIDとともに位置演算部24に出力する。混入された信号としては、マルチバスなどの要因によりやむを得ず混入される場合と、信号発生装置などにより不正に混入される場合が考えられる。前者のマルチバスについては、一般に知られた方式で除去を行う。後者については、信号蓄積部25に記録されている

信号を利用して除去する。例えば、伝送用データからおおよその位置と時刻を算出し、その位置と時刻に近い信号を信号蓄積部25から取り出し比較して、その信号が正しいものかどうかを判定する。ここで正しいものでないと判定された場合には、その信号を除去する。

サーバの位置演算部24は、受け取った伝送用データから位置と時刻を算出し、端末のIDとともに証明書生成部22に出力する。また、受け取った伝送用データと算出された位置、時刻、及び端末に固有のIDを信号蓄積部25に出力し、信号蓄積部25は、受け取ったこれらの値を関連付けて記録する。

#### 【0022】

この構成により、伝送用データに混入された信号を除去することができ、従ってより信頼性の高い位置保証が可能となる効果がある。

#### 【0023】

本実施の形態における他のシステム構成を図8に示す。即ちサーバ20eは、補正情報センタ61が提供する補正情報61bを受信できる。このとき、補正情報61bは通信手段の他に、放送手段にて提供されることもある。

またハードウェア構成としては、図9に示す構成となり、補正情報61bを受信する補正情報受信部27を備える。

#### 【0024】

この構成におけるシステムの動作は、ほとんど実施の形態1と同様であるが、以下の動作が加わる。

サーバ20eは、端末から位置保証要求を受けると、該当する測位端末から送信されたGPS信号からその位置と時刻を算出する。このとき補正情報センタ61から得られる補正情報61bを補正情報受信部27で受信してその位置情報も併用して、位置の補正を行う。この補正の仕方は、通常知られている方式で行う。

#### 【0025】

この構成により、補正情報を利用してより正しい位置情報とするので、精度の高い位置保証可能となる効果がある。

#### 【0026】

本実施の形態における他のシステムを説明する。

システムの構成と、ハードウェア構成は、実施の形態1と同様であるが、サーバ20fは、実施の形態1における証明書生成部22の代わりに、受信した時刻と、算出された位置と、その精度に対する証明書を作成する証明書生成部22Bとする。

#### 【0027】

本構成における動作は、ほとんど実施の形態1と同様であるが、以下の部分が異なる。即ち、サーバの位置演算部24は、受け取った伝送用データから位置とその精度、時刻を算出する。この算出に際して、衛星の配置の良さを示す指標としてG D O P (Geometrical Dilution Of Precision) を用いる。G D O P が小さいほど衛星の配置がよく、測位精度への影響が小さい。このような品質情報も利用して、保証可能な精度を算出する。また、補正を行った場合は、そのときに利用した補正方式に応じて精度を算出する。更に、端末の通信ネットワーク上の位置を利用した場合には、その利用方式に応じて精度を算出する。

サーバの証明書生成部22Bは、受け取った位置とその精度、時刻及び端末のIDに対する証明書を作成する。この証明書は改ざん不可能なものとし、その作成方式は一般に知られている方式を利用する。

#### 【0028】

この構成により、位置だけではなくその精度（含んでいる誤差）も保証できる効果がある。

更に、課金システムに適用した場合、ユーザが必要としている精度に応じた料金を設定することが可能となる。

#### 【図面の簡単な説明】

【0029】

【図1】この発明の実施の形態1におけるシステムのハードウェア構成を示す図である。

【図2】実施の形態1におけるシステム構成を示す図である。

【図3】実施の形態1におけるシステムの動作を示すフロー図である。

【図4】この発明の実施の形態2におけるシステムの構成を示す図である。

【図5】実施の形態2におけるシステムのハードウェア構成を示す図である。

【図6】実施の形態2における他のシステムのハードウェア構成を示す図である。

【図7】この発明の実施の形態3におけるシステムのハードウェア構成を示す図である。

【図8】実施の形態3における他のシステムの構成を示す図である。

【図9】実施の形態3における他のシステムのハードウェア構成を示す図である。

【図10】従来の一般的な測位端末の構成を示す図である。

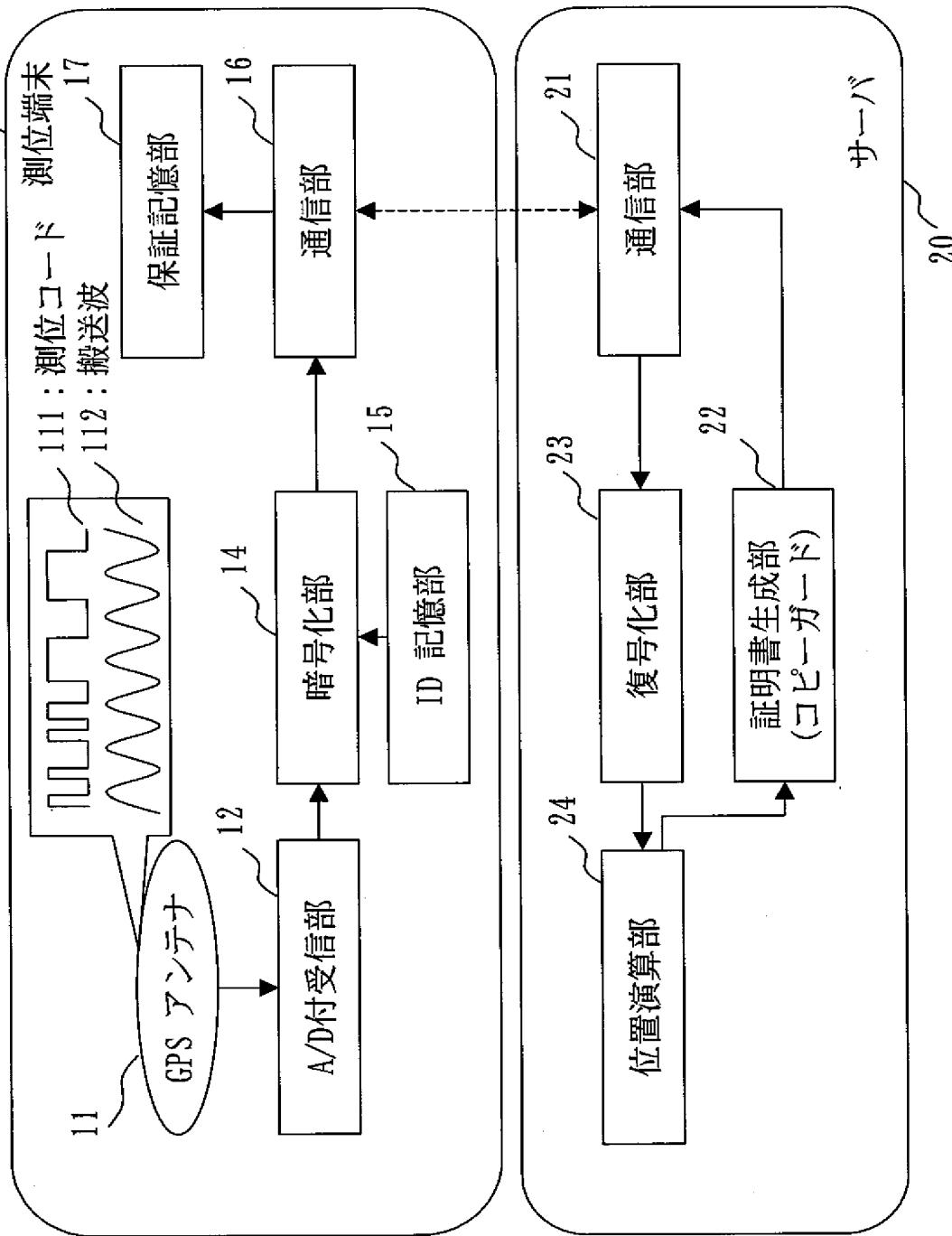
#### 【符号の説明】

【0030】

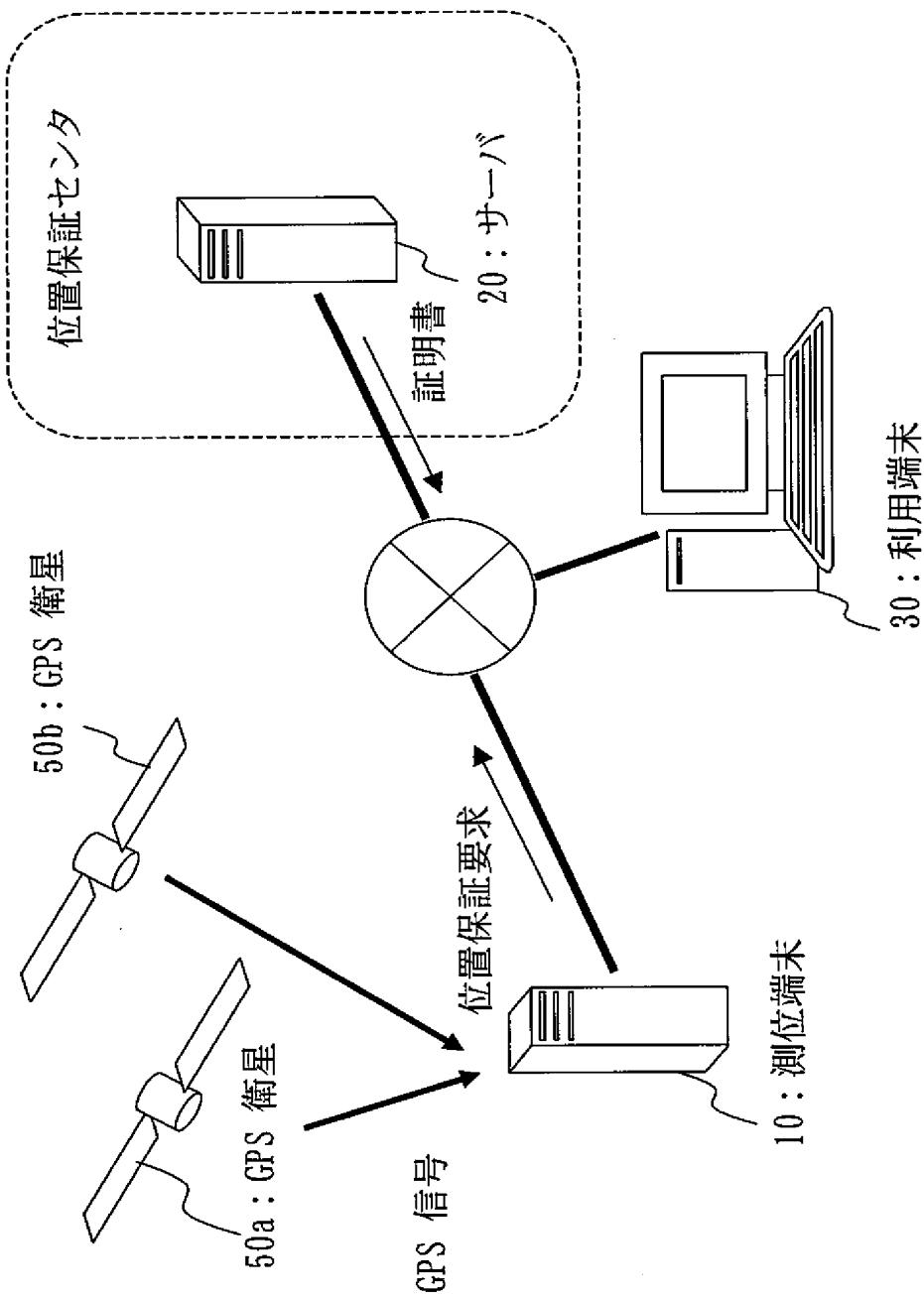
10, 10b, 10c 測位端末、11 GPSアンテナ、12 A/D付受信部、14 暗号化部、15 ID記憶部、16 通信部、17 保証記憶部、18 時刻証明受信部、20, 20d, 20e サーバ、21 通信部、22 証明書生成部、23 復号化部、24 位置演算部、25 信号蓄積部、26 信号除去部、27 補正情報受信部、30 利用端末、31 耐タンパ化部、40 基地局、50a, 50b GPS衛星、51 準天頂衛星、61 補正情報センタ、61b 補正情報、111 測位コード、112 濾送波、S31 位置保証要求受信確認ステップ、S32 測位コード・濾送波の復号ステップ、S33 位置演算ステップ、S34 位置保証書生成ステップ、S41 測位コード・濾送波送信、位置保証要求送信ステップ、S42 位置保証書受信確認ステップ。

【書類名】図面  
【図 1】

10

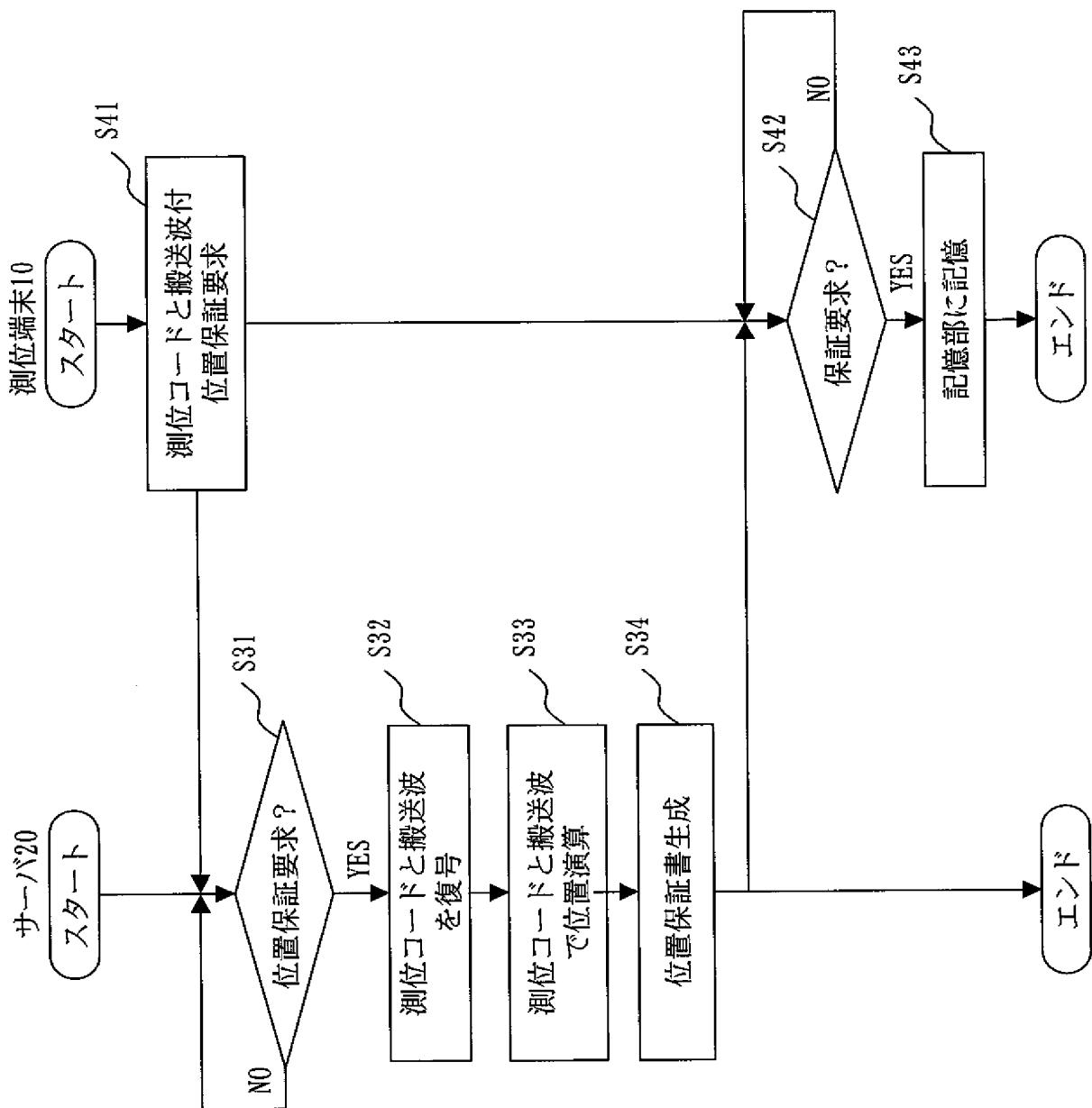


【図 2】

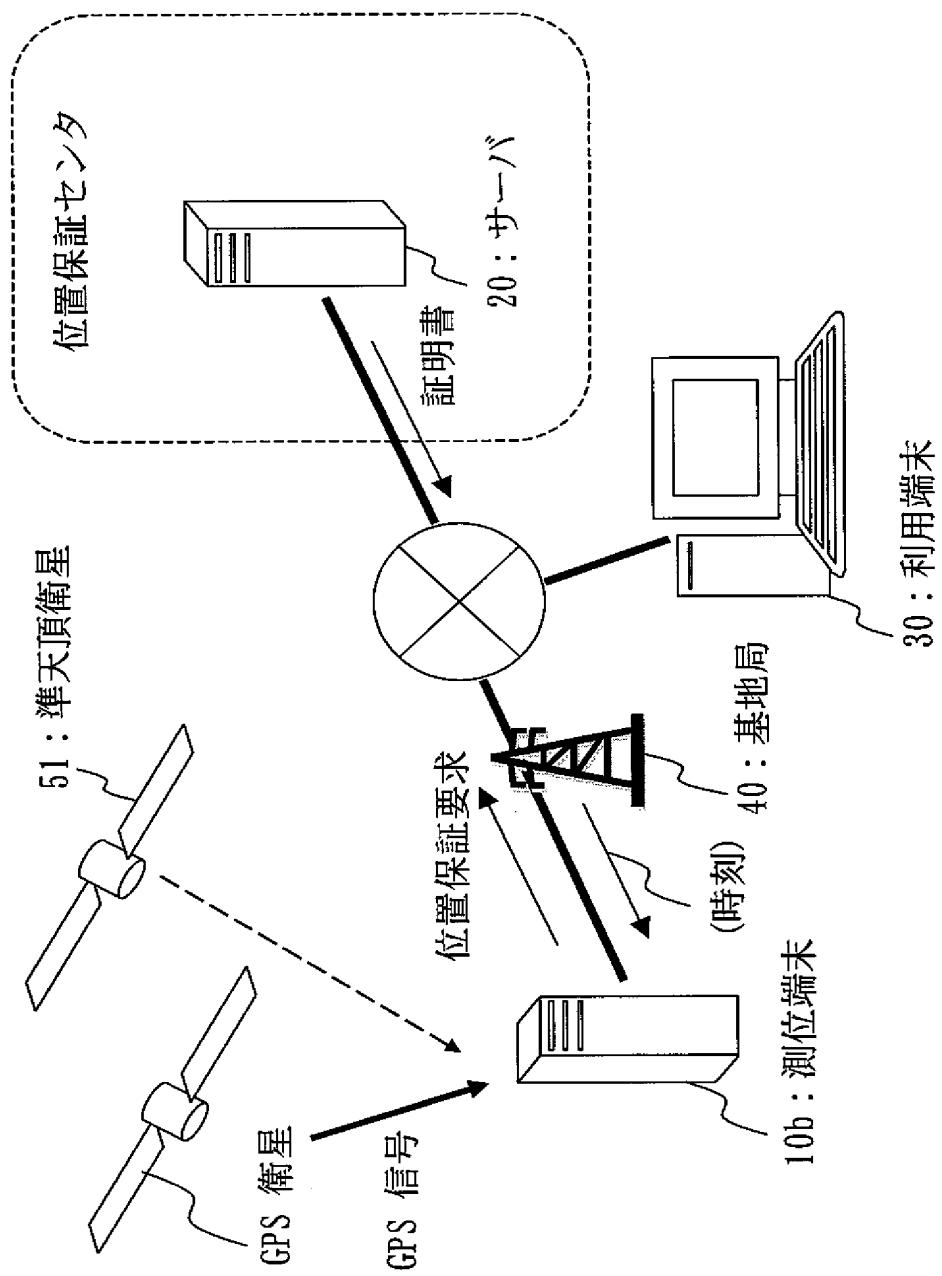


位置保証システムを利用したサービス提供システムの構成例

【図3】



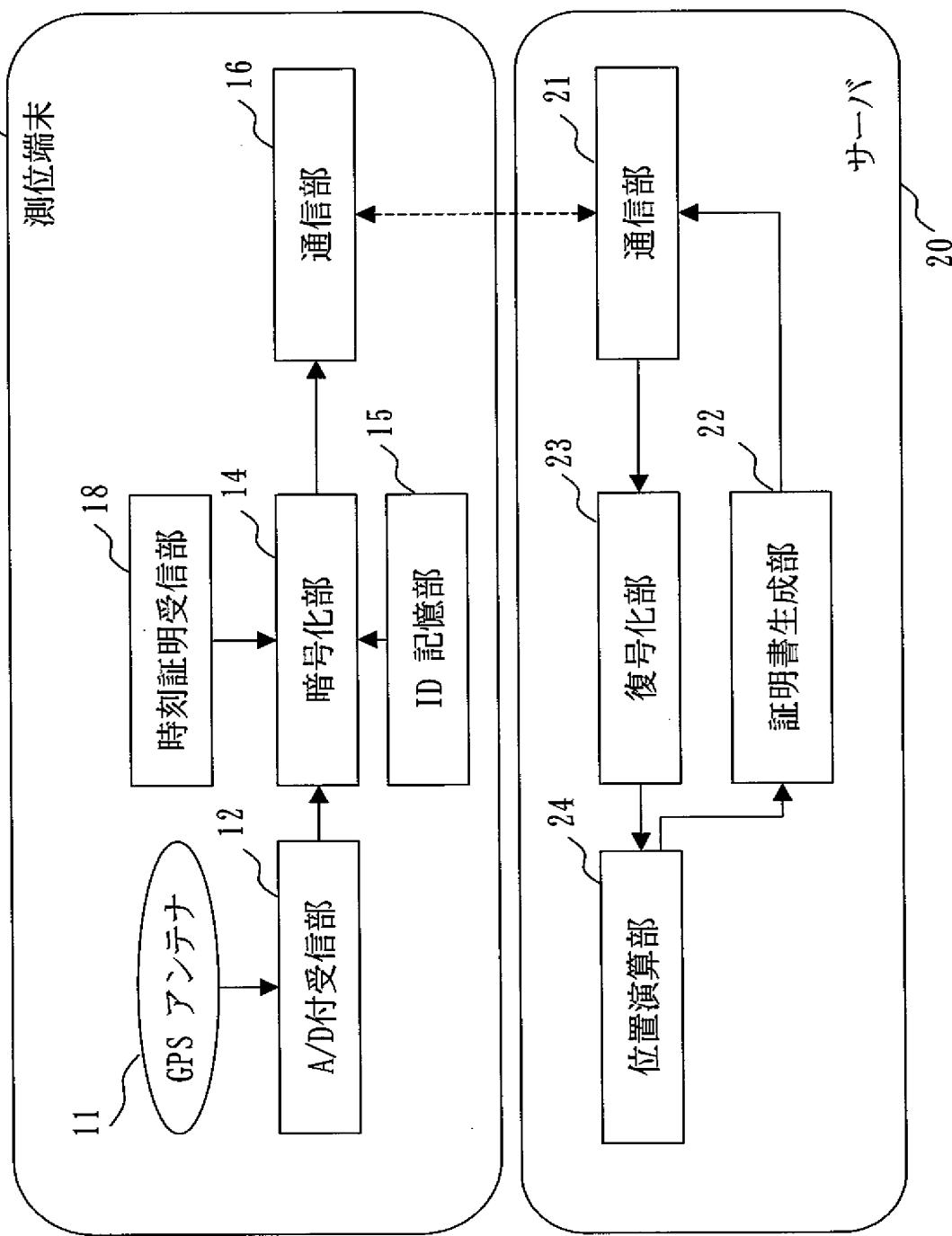
【図 4】



位置保証システムを利用したサービス提供システムの構成例

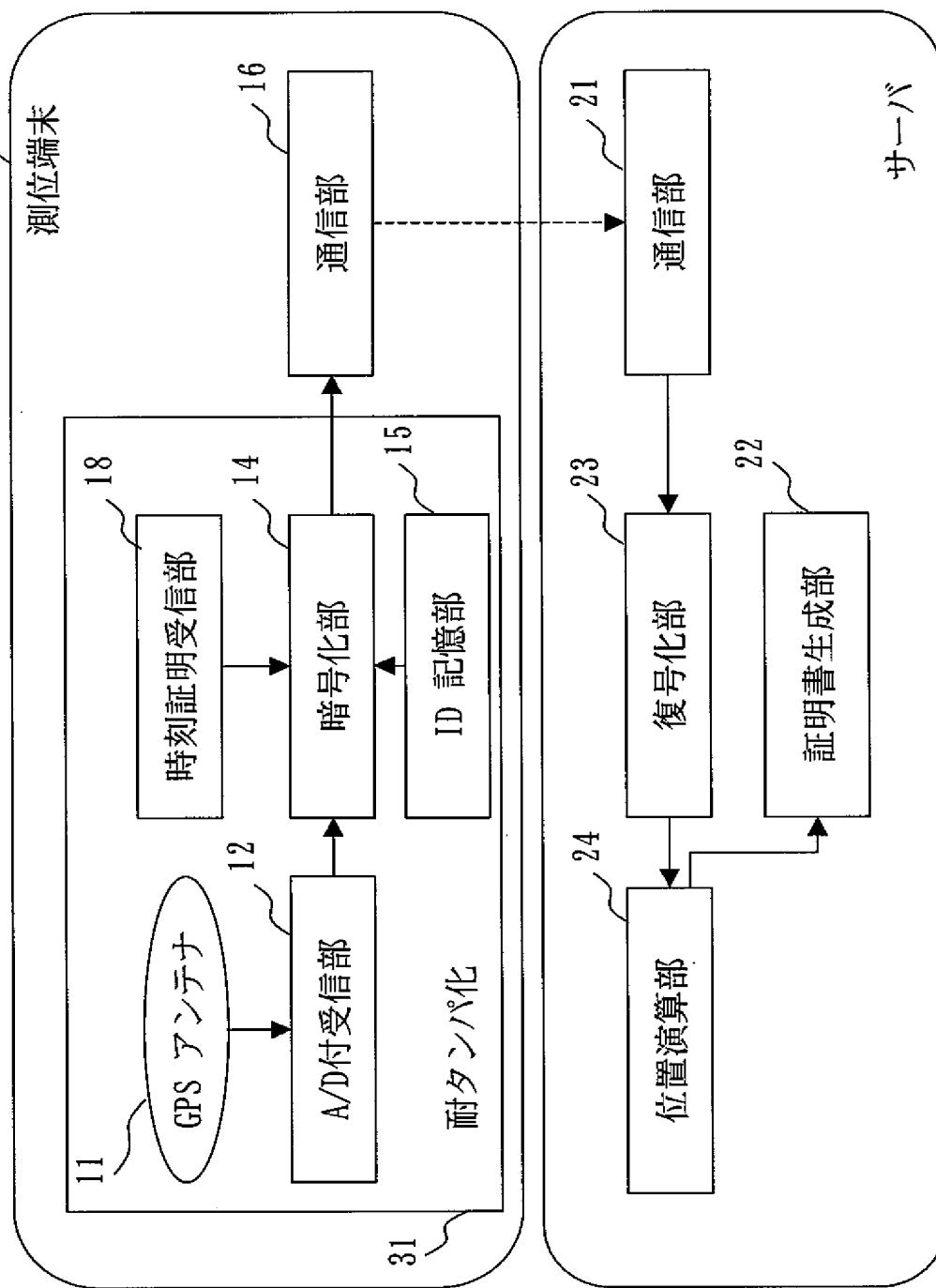
【図 5】

10b

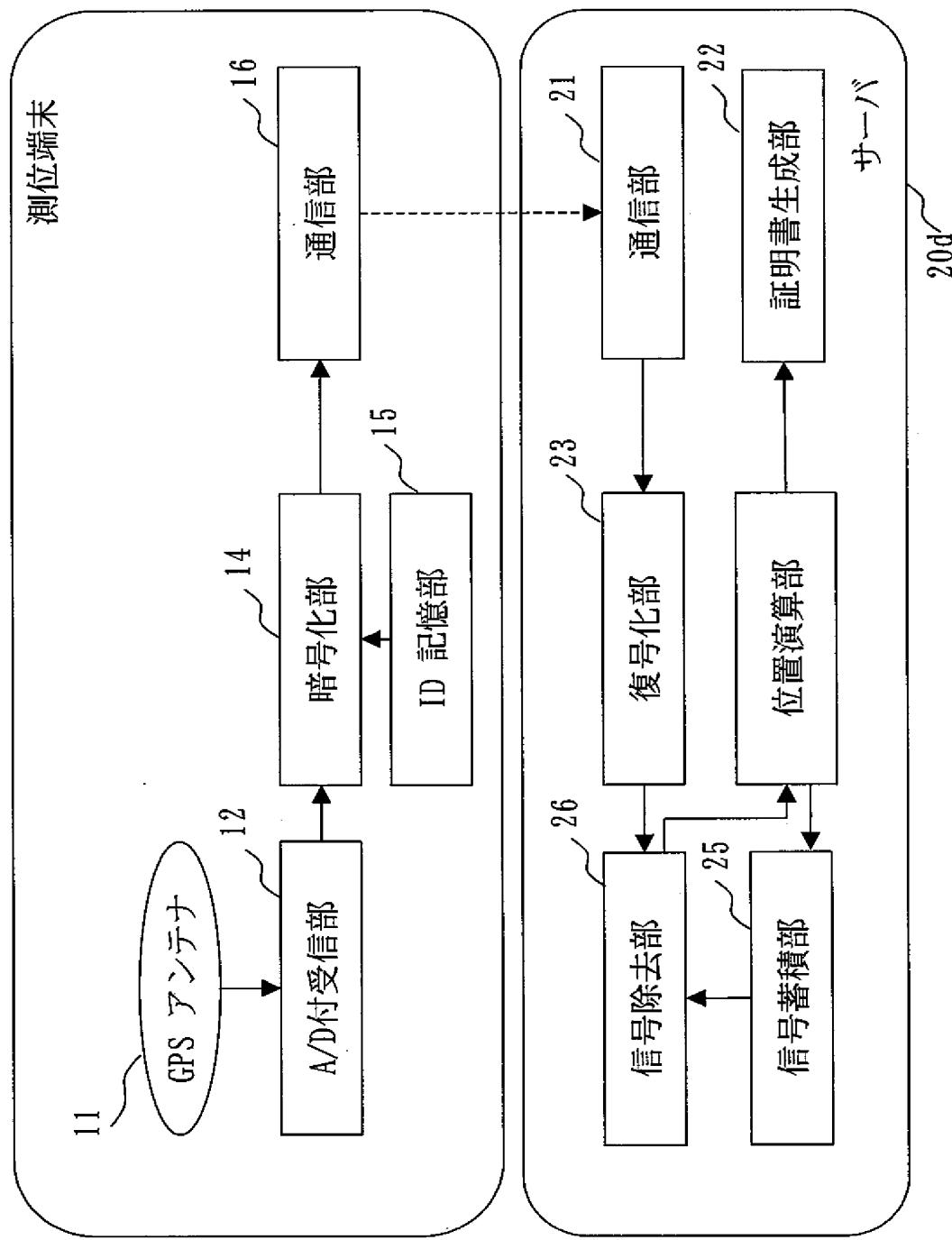


【図6】

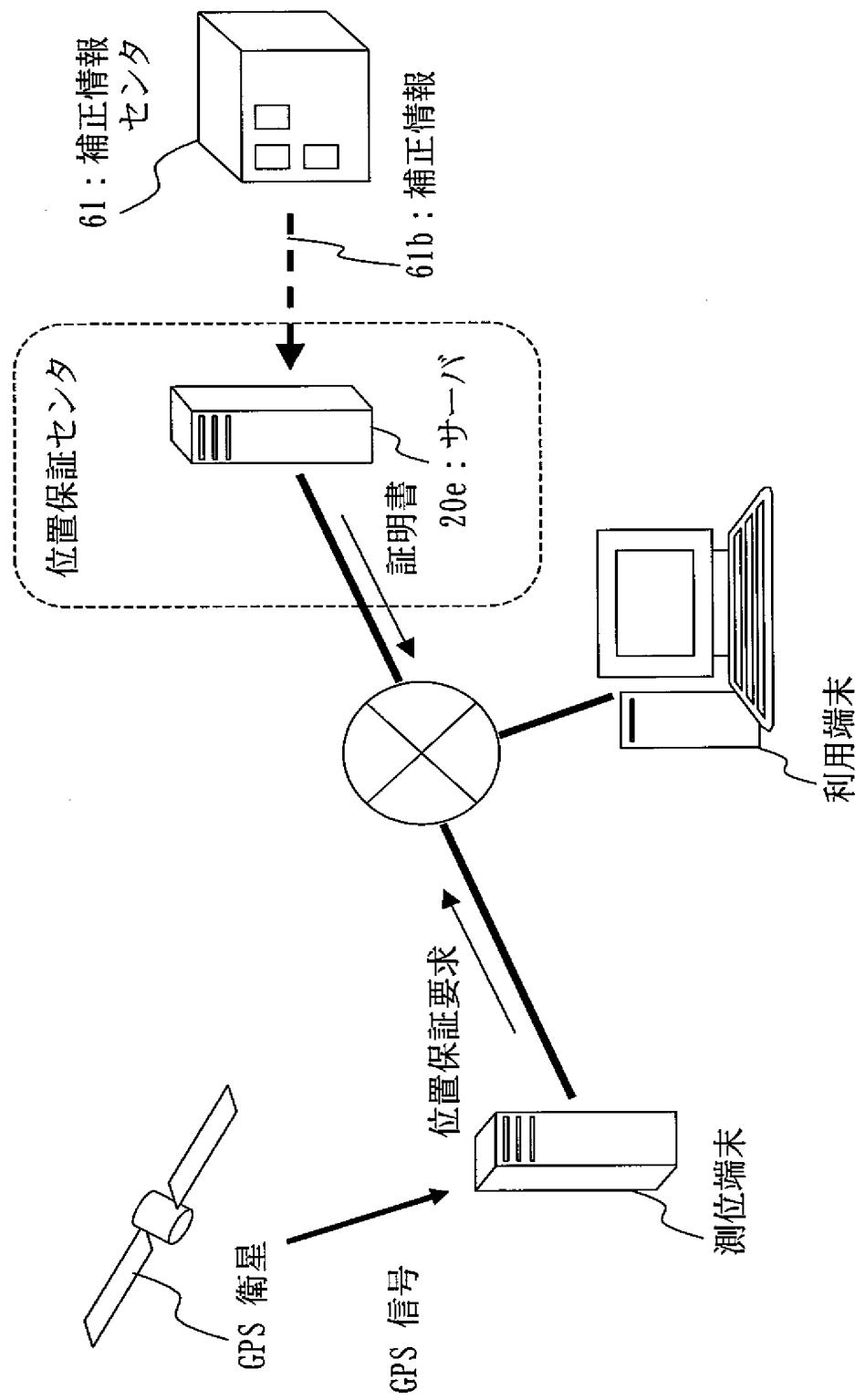
1



【図 7】

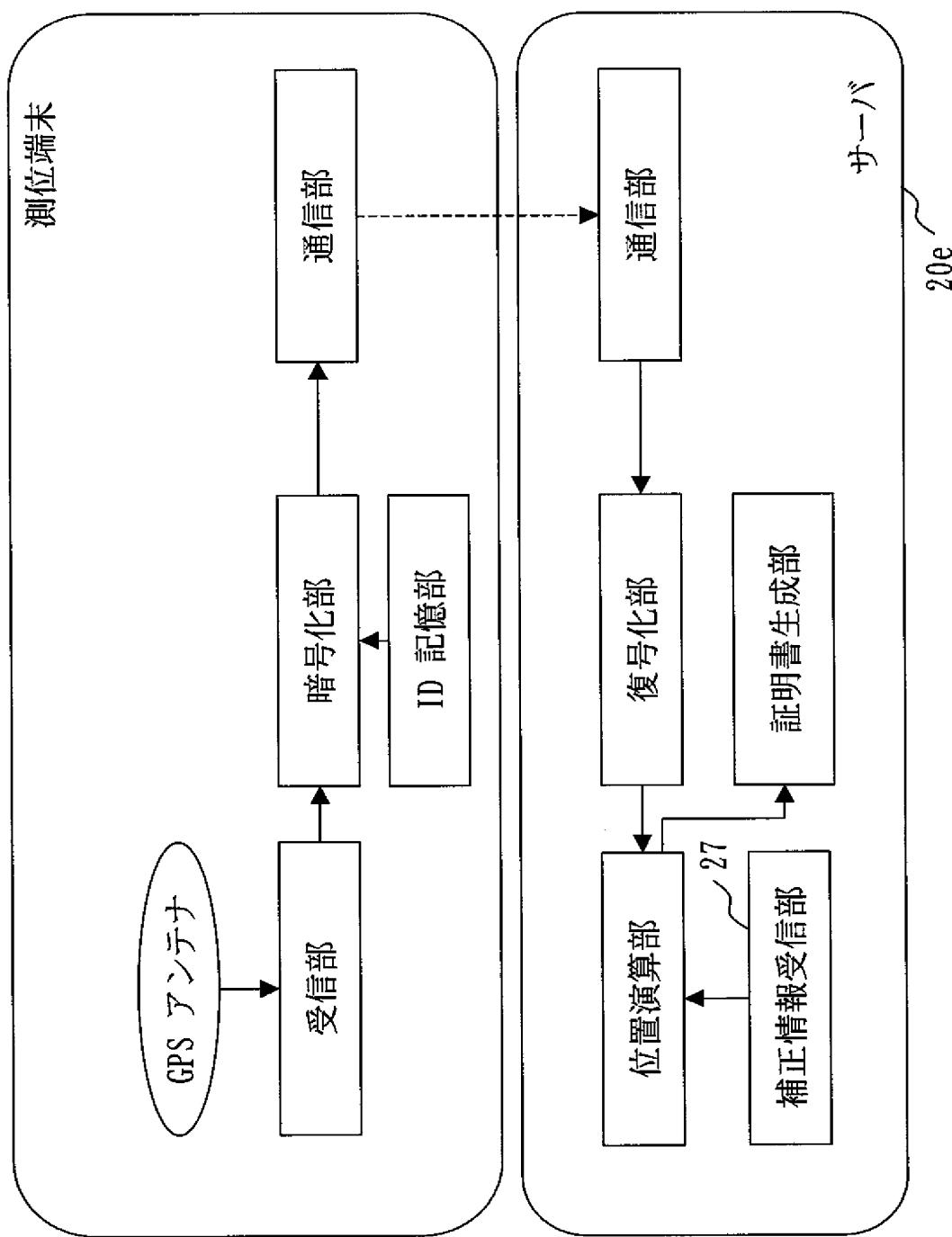


【図 8】

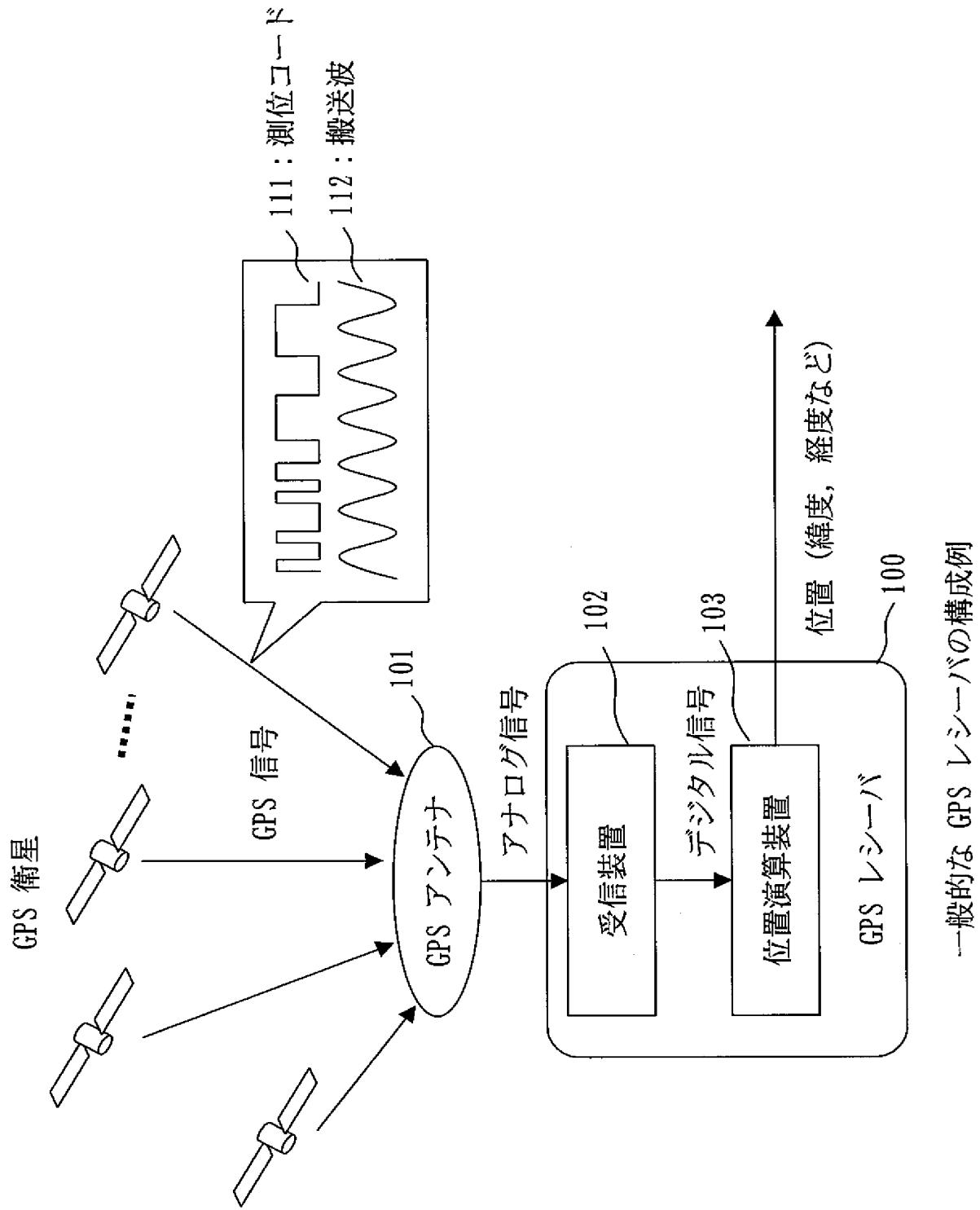


位置保証システムを利用したサービス提供システムの構成例

【図 9】



【図 10】



【書類名】要約書

【要約】

【課題】データの改竄ができにくく、かつ、即時応答が可能で、信頼性の高い位置保証を得る。

【解決手段】測位衛星からの測位コードと搬送波とを自身の識別符号で暗号化して測位端末から送信された伝送データを受信して、上記測位端末の識別符号を記憶して、該識別符号で上記伝送データを復号化する復号化部23と、上記復号化部によって復号化された測位コードと搬送波とに基づいて上記測位端末の位置を演算する位置演算部24と、上記位置演算で得られた位置情報を証明する証明書生成部22とを備えて、端末から位置保証要求があると、該当する上記位置演算による位置情報の証明を行うことを特徴とする。

【選択図】

図 1

出願人履歴

0 0 0 0 0 6 0 1 3

19900824

新規登録

5 9 1 0 3 1 9 2 4

東京都千代田区丸の内 2 丁目 2 番 3 号

三菱電機株式会社